

Cisco Small Business Router Password Disclosure Vulnerability

Advisory ID: cisco-sa-20140305-rpd

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140305-rpd>

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

Revision 1.0

For Public Release 2014 March 5 16:00 UTC (GMT)

目次

- [要約](#)
- [該当製品](#)
- [詳細](#)
- [脆弱性スコア詳細](#)
- [影響](#)
- [ソフトウェア バージョンおよび修正](#)
- [回避策](#)
- [修正済みソフトウェアの入手](#)
- [不正利用事例と公式発表](#)
- [この通知のステータス: FINAL](#)
- [情報配信](#)
- [更新履歴](#)
- [シスコ セキュリティ手順](#)

要約

Cisco RV110W Wireless-N VPN ファイアウォール、Cisco RV215W Wireless-N VPN ルータ、Cisco CVR100W Wireless-N VPN ルータの Web 管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスの Web 管理インターフェイスへの管理者レベルのアクセス権を取得できる可能性があります。

この脆弱性は、Web フレームワークによる、認証要求の不適切な処理に起因します。攻撃者は、認証要求の傍受、変更、再送信によって、この脆弱性を不正利用する可能性があります。この脆弱性による不正利用が成功すると、攻撃者は該当デバイスの Web ベースの管理インターフェイスに管理者レベルでアクセスできる可能性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。現在、この脆弱性を軽減する既知の回避策はありません。このアドバイザリは、次のリンクで確認できます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140305-rpd>

該当製品

脆弱性が認められる製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けます。

- ファームウェア バージョン 1.2.0.9 以前を実行している Cisco RV110W Wireless-N VPN ファイアウォール
- ファームウェア バージョン 1.1.0.5 以前を実行している Cisco RV215W Wireless-N VPN ルータ
- ファームウェア バージョン 1.0.1.19 以前を実行している Cisco CVR100W Wireless-N VPN ルータ

脆弱性が認められない製品

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco RV110W Wireless-N VPN ファイアウォール、Cisco RV215W Wireless-N VPN ルータ、Cisco CVR100W Wireless-N VPN ルータの Web 管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスの Web 管理インターフェイスへの管理者レベルのアクセス権を取得できる可能性があります。

この脆弱性は、Web フレームワークによる、認証要求の不適切な処理に起因します。攻撃者は、認証要求の傍受、変更、再送信によって、この脆弱性を不正利用する可能性があります。この脆弱性による不正利用が成功すると、攻撃者は該当デバイスの Web ベースの管理インターフェイスに管理者レベルでアクセスできる可能性があります。

この脆弱性は、Cisco Bug ID [CSCuI94527](#) ([登録ユーザ専用](#))、[CSCum86264](#) ([登録ユーザ専用](#)) および [CSCum86275](#) ([登録ユーザ専用](#)) として文書化され、Common Vulnerabilities and Exposures として CVE-2014-0683 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System (CVSS) に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア (Base Score) および現状評価スコア (Temporal Score) を提供しています。お客様はこれらを用いて環境評価スコア (Environmental Score) を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンク

で提供しています。

<http://tools.cisco.com/security/center/cvssCalculator.x/>

CSCuI94527, CSCum86264 and CSCum86275 Cisco Small Business Router Password Disclosure Vulnerability Calculate the environmental score of					
CVSS Base Score - 10.0					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、攻撃者は該当デバイスの完全な制御権を取得できる可能性があります。完全な管理者権限でデバイスにアクセスする攻撃者は、Web ベースの管理ユーザインターフェイスを介してルータのすべての設定を行えるようになります。

ソフトウェア バージョンおよび修正

シスコは、このアドバイザリに記載されている脆弱性に対応するための無償ソフトウェア アップデートをリリースしました。

Cisco CVR100W Wireless-N VPN ルータ ファームウェア バージョン 1.0.1.21 :

<http://software.cisco.com/download/release.html?mdfid=284758089&flowid=43303&softwareid=282487380&release=1.0.1.21&reind=AVAILABLE&rellifecycle=&reltype=latest>

Cisco RV110W Wireless-N VPN ファイアウォール ファームウェア バージョン 1.2.0.10 :

<http://software.cisco.com/download/release.html?mdfid=283879340&softwareid=282487380&release=1.2.0.10&reind=AVAILABLE&rellifecycle=&reltype=latest>

Cisco RV215W Wireless-N VPN ルータ ファームウェア バージョン 1.1.0.6 :

<http://software.cisco.com/download/release.html?mdfid=284436489&softwareid=282487380&release=1.1.0.6&reind=AVAILABLE&rellifecycle=&reltype=latest&i=rm>

ソフトウェアのアップグレードを検討する場合は、<http://www.cisco.com/go/psirt/> の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

回避策

現時点で使用可能な既知の回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャンネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、[Cisco.com](http://www.cisco.com) の Software Navigator からアップグレードを入手することができます。 <http://www.cisco.com/cisco/software/navigator.html>

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center (TAC) に連絡してアップグレード ソフトウェアを入手してください。

• +1 800 553 2447 (北米からの無料通話)

- +1 408 526 7209 (北米以外からの有料通話)
- E メール : tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先 (http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) を参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

この脆弱性をご報告いただいた Gustavo Javier Speranza 氏に感謝いたします。

この通知のステータス : FINAL

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証を示唆するものでもありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意識を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140305-rpd>

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信さ

れるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-March-05	Initial public release
--------------	---------------	------------------------

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、<http://www.cisco.com/go/psirt/> で確認することができます。